Abstract of the Disclosure

A biometrically secured memory IC is disclosed for biometrically securing digital data stored therein. The memory IC comprises a biometric sensing device such as a fingerprint imager and an integrated circuit. The biometric sensing device and the integrated circuit are irremovably bonded together such that the sensing device and the integrated circuit form a single physical unit. Biometric information provided to the sensing device is captured and a signal indicative of the biometric information is provided to the integrated circuit. The signal is then converted into digital data indicative of the signal using an A/D converter. A processor compares the digital data indicative of the biometric information with first digital data indicative of a biometric characteristic of an authorized user, which is stored in first memory to produce a comparison result. If the comparison result is indicative of a match the processor provides access to second digital data stored in second memory. The integrated circuit further comprises a port for providing and/or receiving second digital data. The circuitry for the A/D converter, the processor, first memory and second memory are all contained within a single integrated circuit. With an aspect of the invention there is further disclosed a method for copying second digital data from a first biometrically secured memory IC to a second void biometrically secured memory IC. The combination of the data storage as well as the biometric security system in a single unit such as a chip provides a substantially tamperproof device making it next to impossible to access the data without destroying the device.